CLAIMS

What is claimed is:

1. A method for conducting a transaction, the method comprising:
   a. receiving a transaction request from a user at a server;
   b. issuing a challenge to the user;
   c. receiving a response from the user based upon said challenge;
   d. processing said response to verify an instrument;
   e. assembling credentials for the transaction, said credentials comprising at least one key;
   f. providing at least a portion of said credentials to said user;
   g. receiving a second request from said user, said second request including said portion of said credentials; and
   h. validating said portion of said credentials with said key to provide access to a transaction service.

2. The method of Claim 1, wherein the transaction is an electronic purchase transaction.

3. The method of Claim 2, wherein the electronic purchase transaction is conducted using a digital wallet.

4. The method of Claim 1, wherein the instrument is a smartcard.

5. A method for protecting a network server from being used as the basis of an attack on a network client, the method comprising:
   a. restricting access to said network server to a portion of said network server for at least a selected protocol; and
   b. scanning said portion of said network server for particular characters, said particular characters being associated with said selected protocol.

6. The method of Claim 5, further comprising removing said particular characters such that a security risk posed by said selected protocol is reduced.

7. The method of Claim 5, further comprising replacing said particular characters with benign characters such that a security risk posed by said selected protocol is reduced.

8. The method of Claim 5, wherein said characters are hostile characters and wherein if a request contains any of said hostile characters, the request is rejected.

9. The method of Claim 5, further comprising logging said particular characters to form a security log.

10. The method of Claim 9, further comprising reviewing said security log to determine whether said particular characters are hostile.

11. The method of Claim 5, wherein said protection of the network server is accomplished during an electronic purchase transaction.

12. The method of Claim 11, wherein the electronic purchase transaction is conducted using a digital wallet.

13. A transaction system, wherein the transaction system comprises:

a. a user computer, wherein said user computer is operated by a user;

b. a transaction authorizer computer;

c. a data network, wherein when the user wishes to execute a transaction, a connection is established between said user computer and said transaction authorizer computer via said data network; and

d. a security server, wherein a connection is established between said security server and said user computer to verify that an intelligent token is in the user's possession.

14. The transaction system of Claim 13, further comprising a transaction tool server.

15. The transaction system of Claim 13, wherein the user is a purchaser, the transaction authorizer is a merchant and the user and merchant consummate a purchase transaction.

16. The transaction system of Claim 15, further comprising a wallet server.

17. The transaction system of Claim 13, wherein the user computer comprises a transaction tool and a reader, wherein said reader is capable of transferring information between the transaction tool and the intelligent token.

18. The transaction system of Claim 17, wherein said transaction tool is a wallet client.

19. The transaction system of Claim 13, wherein the intelligent token is a smartcard.

20. The transaction system of Claim 13, wherein the connection between said security server and said transaction authorizer computer is through a data connection separate from said data network.

21. The transaction system of Claim 17, wherein said transaction tool communicates with said security server via a data connection separate from said data network.

22. The transaction system of Claim 13, wherein the intelligent token comprises a digital certificate that uniquely identifies the user associated with the intelligent token.

23. The transaction system of Claim 22, wherein the user of said intelligent token unlocks access to the digital certificate by use of a personal identifier.

24. The transaction system of Claim 13, wherein the intelligent token is issued by an issuer and wherein a transaction made using said transaction system is considered a "card present" transaction as deemed by the issuer of the intelligent token.

25. A digital wallet comprising:
    a. at least one server; and
    b. an activator for accessing said at least one server, wherein said activator exchanges information with said at least one server.

26. The digital wallet of Claim 25, wherein said at least one server includes a digital wallet server.

27. The digital wallet of Claim 25, wherein said at least one server includes at least one non-wallet application.

28. The digital wallet of Claim 25, wherein a client window is displayed in a browser window.

29. The digital wallet of Claim 25 further comprising a toolbar.

30. A digital wallet comprising:
    a. at least one server; and
    b. a toolbar.

31. The digital wallet of Claim 30, wherein said digital wallet further comprises an activator.

32. The digital wallet of Claim 31, wherein said toolbar performs a small download of said activator.

33. The digital wallet of Claim 30, wherein said toolbar utilizes an operating system control element.

34. The digital wallet of Claim 33, wherein the operating system control element is a system tray icon.

35. The digital wallet of Claim 30, further comprising a transaction authorizer window.

36. The digital wallet of Claim 35, wherein said toolbar is a discrete window that associates with the transaction authorizer window.

37. The digital wallet of Claim 30, further comprising a form fill component which allows a user to pre-fill forms.

38. The digital wallet of Claim 37, wherein the form fill component comprises a model that characterizes a transaction authorizer site.

39. The digital wallet of Claim 37, wherein the form fill component comprises a model that characterizes a user.

40. The digital wallet of Claim 37, wherein the form fill component comprises:

a. a model that characterizes a transaction authorizer site; and

b. a model that characterizes a user.

41. The digital wallet of Claim 30, further comprising an auto-remember component.

42. The digital wallet of Claim 36, wherein the auto-remember component includes heuristics based field recognition.

Add A1